



Personal Health Information Protection Act, 2004



Children's Mental Health Ontario
Santé Mentale pour Enfants Ontario

40 St. Clair Ave. E., Suite 309, Toronto, Ontario M4T 1M9
Tel: 416-921-2109 • Fax: 416-921-7600 • www.kidsmentalhealth.ca

Ken Anderson
Assistant Commissioner (Privacy)
Information and Privacy Commissioner
Ontario

November 27, 2007



PRIVACY DEFINED

Informational Privacy: Data Protection

- Freedom of choice, personal control, informational self-determination;
- Control over the collection, use and disclosure of recorded information about an identifiable individual;
- An organization's responsibility for data protection and the safeguarding of personally identifiable information, in its custody or control.



Canada's Fair Information Practices

- **Accountability**
- **Identifying Purposes**
- **Consent**
- **Limiting Collection**
- **Limiting Use,
Disclosure, Retention**
- **Accuracy**
- **Safeguards**
- **Openness**
- **Individual Access**
- **Challenging**
- **Compliance**

CSA Model Code for the Protection of Personal Information
(Privacy Code) CAN-CSA Q830 1996

www.csa.ca/standards/privacy/code/



Personal Health Information Protection Act (PHIPA)

- Applies to organizations and individuals involved in the delivery of health care services in both the public and private sectors;
- The only health sector privacy legislation in Canada based on consent: implied consent within the “circle of care,” otherwise, express consent;
- The only health sector privacy legislation that was declared to be substantially similar to the federal *PIPEDA* legislation, in 2005;
- The only legislation in Canada with a mandatory breach notification requirement.



Stressing the 3 C's

Consultation

- Opening the lines of communication with the health care sector and seeking their views.

Co-operation

- Not confrontation in resolving complaints taking a non-adversarial approach.

Collaboration

- Working together to find joint solutions.



Building A Culture of Privacy

- A culture of privacy enables sustainable action throughout an organization by providing people with a similarity of approach, outlook, and priorities;
- The importance of privacy must be a message that comes from the top;
- One way of getting the message across is by devoting adequate resources to privacy programs;
- Privacy must be woven into the fabric of the day-to-day operations of an organization.



Organizational Culture

As a group acquires history, it acquires culture

Edgar Schein, *Organizational Culture and Leadership*, 1988

Culture: patterns of basic assumptions considered correct way to deal with problems

In new situations, culture can turn from powerful capability into powerful disability

Adaptation/transformation can be required



Cultural Transformation

- Cultural change is made of many small changes
- Business sector filled with blueprints for change
- Business books filled with barriers to change
- Two common factors for success:

Passion & Board Support



Privacy and Culture?

"If the predominant concerns of contemporary North American culture have to do with individual autonomy, privacy, security and survival, then reality-based programming seems to respond on all fronts“.

National Post

Dr. Gabriele Helms

Professor of English

University of British Columbia



Privacy Culture Organizations?

- RBC which actually measures importance of privacy to the bottom line of the bank
- ICES which sets a very high standard for privacy and health research
- Ontario's Workplace Safety & Insurance Board which began their transformation January 2002
- Two Ontario government ministries working on this currently + Ontario's CPO is an advocate



What Does A Privacy Culture Look Like?

Accounting for Privacy Like Money

- Treating data as a very important asset
- Conducting full training of all staff
- Personnel bonding
- Audit time/cost built into the system
- Constantly re-enforcing HR: hiring, evaluation
- Planning and practicing for data-loss events

Curt Franklin
University of Florida



Weaving Privacy into Day-to-Day Operations

- On-going privacy training and awareness program (new staff training; refresher training for existing staff, identifying new threats to privacy, finding new technology solutions);
- Policies and procedures for maintaining privacy must be clearly articulated, and individuals must know how to apply them in their day-to-day work;
- Privacy must form part of the performance standard for individuals working in the information-intensive health care sector.



PHIPA OVERVIEW

TOOLS TO HELP STAFF

- We have many informative documents on our web site that could be used in a training program, such as our “A Guide to the Personal Health Information Protection Act” as well as many fact sheets and other guidelines.
- Additionally, our Orders and Reports dealing with PHIPA have educational value. We have a PHIPA video that is available free of charge.
- We do have links to two helpful Toolkits for dealing with PHIPA, on our web site - a Physicians Toolkit and a Hospital Toolkit.
- One that may be more relevant for them was developed by a consultant to the Canadian Mental Health Association. It can be found at: www.ontario.cmha.ca/privacytoolkit/index.asp




“Portable Files”

- Many jobs require records containing personal health information to be taken for work purposes outside of the office
 - Hard copy or electronic files to be used by nurses, case workers, doctors, researchers, CCAC
- How should professionals protect personal health information when carrying it and accessing it outside the office?



Encrypting Personal Health Information on Mobile Devices

- Why are login passwords not enough?
- What is encryption?
- What are the options?
 - Whole disk (drive) encryption
 - Virtual disk encryption
 - Folder or Directory encryption
 - Device encryption
 - Enterprise encryption



Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 12
May 2007

Encrypting Personal Health Information on Mobile Devices

Section 12 (1) of the *Personal Health Information Protection Act, 2004 (PHIPA)* sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

The Office of the Information and Privacy Commissioner/Ontario recognizes that the delivery of health care may require the use of PHI outside of the workplace, and that such PHI may most effectively be transported and used in electronic form. Notwithstanding the ease of use and portability of electronic documents, it is still important that only the minimum necessary data be transported in this manner.

Because of the high incidence of loss or theft of mobile devices such as laptop computers, personal digital assistants (PDAs), or flash drives, custodians need to ensure that personal health information that is stored on mobile devices is encrypted. When encryption is implemented properly, it renders PHI safe from disclosure. The availability of encryption means that it is easier to safeguard electronic records of PHI than it is to safeguard paper-based records when being transported.

This fact sheet is intended for health information custodians who store PHI on mobile devices. However, it is also relevant to anyone who stores personal information on a mobile device. If you are unsure of the meaning of these guidelines, please consult a computer systems security expert to determine how to apply this fact sheet to the information in your care. In many cases, encryption can be as easy as installing a simple program and implementing proper key management for the system.

Why are login passwords not enough?

It is not acceptable to rely solely on login passwords to protect PHI on devices that are easily stolen or lost. "Strong" login passwords will prevent casual access to data on a device, but may not prevent access by knowledgeable thieves. Strong login passwords are usually characterized by:

- No dictionary words;
- A combination of letters, numbers and symbols;
- Eight or more characters, with 14 or more being ideal.

For example, "LetMeIn" is a weak password because it uses dictionary words. On the other hand, you could remember the phrase, "My birthday is October 21 and I'm 25"



DE-PERIMETERIZATION

- This is a term used in the areas of information security, IT security, network security and computer security.
- De-perimeterization is a concept/strategy used to describe protecting an organization's systems and data on multiple levels by using a mixture of encryption, inherently-secure computer protocols, inherently-secure computer systems and data-level authentication rather than the reliance of an organization on its (network) boundary to the Internet.
- For the health sector, this is like “universal precautions”.



DE-PERIMETERIZATION

Successful implementation of a de-perimeterized strategy within an organization implies that the perimeter or outer security boundary, could be removed.





Health Order No. 5

Wireless Technology Results in Order

- **Health Order No. 5** (HO-05) resulted from a methadone clinic that installed a wireless video surveillance system in its washroom to monitor patients providing urine samples;
- Video images were intercepted by a wireless rear view backup camera in a car outside of the clinic;
- The Clinic was ordered to strongly encrypt all wireless signals if wireless video technology was to be utilized, and to review encryption practices on an annual basis;
- The standard of practice created by this Order was that if healthcare providers choose to use wireless technology, then they must encrypt – strongly.



Fact Sheet:

Wireless Communication Technologies

- Special precautions must be taken to protect the privacy of video images;
- No covert surveillance should be conducted;
- Clearly visible signs should be posted indicating the presence of cameras and the location of their use;
- Recording devices should not be used;
- Only minimum number of staff should have access to the video equipment;
- Staff should receive technical training on the privacy and security issues;
- Regular security and privacy audits should be conducted, on an annual basis.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 13
June 2007

**Wireless Communication Technologies:
Video Surveillance Systems**

Section 12(1) of the *Personal Health Information Protection Act (PHIPA)* sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

In a widely publicized incident, for which an Order was issued – HO-005 – images of a patient giving a urine sample in a washroom were being accessed by a wireless mobile rear-assist parking device ("back up camera"), in a car parked near a clinic. The patient was attending a methadone clinic in which patients were required to give urine samples under direct observation. The clinic was unaware that such an interception was even possible.

Closed Circuit Television (CCTV) or video surveillance cameras are being used in the Ontario health sector for a range of purposes ranging from building security to observational research. Typically, these uses increase efficiency or help prevent negative patient outcomes. The unintended consequence of video surveillance, however, regardless of its primary function, is often an invasion of personal privacy. This risk is increased if wireless communication technology is used without adequate protection.

This fact sheet is intended to address privacy issues that arise from the use of wireless communication technologies. The standard established in Order HO-005 is that health information custodians in Ontario should not use wireless video surveillance cameras without strong security and privacy precautions. Any organization that chooses to use wireless communication technology to transmit personally identifiable information needs to take appropriate proactive measures to protect the privacy of individuals.


What is wireless video surveillance technology?

Wireless video surveillance systems, or wireless CCTV, typically refer to systems that transmit wireless signals to television monitors, not computer screens. The most common commercial use of this equipment is for building security. Commercially available systems do not normally have privacy or security designed into the transmission of the signal. As a result, such systems are easy to install but will allow unauthorized access unless special precautions are taken. Health information custodians must ensure that no one other than specifically authorized staff have the capability of viewing patient images.



Encrypting Personal Health Information on Mobile Devices

- Why are login passwords not enough?
- What is encryption?
- What are the options?
 - Whole disk (drive) encryption
 - Virtual disk encryption
 - Folder or Directory encryption
 - Device encryption
 - Enterprise encryption



Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 12
May 2007

Encrypting Personal Health Information on Mobile Devices

Section 12 (1) of the *Personal Health Information Protection Act, 2004 (PHIPA)* sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

The Office of the Information and Privacy Commissioner/Ontario recognizes that the delivery of health care may require the use of PHI outside of the workplace, and that such PHI may most effectively be transported and used in electronic form. Notwithstanding the ease of use and portability of electronic documents, it is still important that only the minimum necessary data be transported in this manner.

Because of the high incidence of loss or theft of mobile devices such as laptop computers, personal digital assistants (PDAs), or flash drives, custodians need to ensure that personal health information that is stored on mobile devices is encrypted. When encryption is implemented properly, it renders PHI safe from disclosure. The availability of encryption means that it is easier to safeguard electronic records of PHI than it is to safeguard paper-based records when being transported.

This fact sheet is intended for health information custodians who store PHI on mobile devices. However, it is also relevant to anyone who stores personal information on a mobile device. If you are unsure of the meaning of these guidelines, please consult a computer systems security expert to determine how to apply this fact sheet to the information in your care. In many cases, encryption can be as easy as installing a simple program and implementing proper key management for the system.

Why are login passwords not enough?

It is not acceptable to rely solely on login passwords to protect PHI on devices that are easily stolen or lost. "Strong" login passwords will prevent casual access to data on a device, but may not prevent access by knowledgeable thieves. Strong login passwords are usually characterized by:

- No dictionary words;
- A combination of letters, numbers and symbols;
- Eight or more characters, with 14 or more being ideal.

For example, "LetMeIn" is a weak password because it uses dictionary words. On the other hand, you could remember the phrase, "My birthday is October 21 and I'm 25"



PHIPA OVERVIEW

Consent

- PHIPA does not deal with consent to treatment. It's focus is on consent to collection, use and disclosure of personal health information. (PHI)
- The assessment of capacity is not dependent upon age per se, but whether to consent and to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing consent.



PHIPA OVERVIEW

Consent

- If a person is less than 16 years of age, a parent (or a children's aid society et al – see S.23) may consent in the their place, except where:
 - a) The information relates to treatment about which the child has made their own treatment decision in accordance with the Health Care Consent Act, or
 - b) Counselling in which the child has participated on his or her own under the Child and Family Services Act.



PHIPA OVERVIEW

Consent

- SS.23(3) of PHIPA provides that if a child, who is less than 16 years of age, is capable of consenting, then that child's decision prevails over that of a substitute decision-maker, which conflicts with the child's.
- Although not stated, in PHIPA, in light of the capacity test and the provision in ss.23(3), we believe it is a best practice for health information custodians (HIC's) to ask children under 16 years of age, who appear capable, if they want to make the decision in regard to collection, use, disclosure, etc., of their PHI.



PHIPA OVERVIEW

Consent

- Under the direction of s.16(5) of the Divorce Act and s.20(5) of the Children’s Law Reform Act, an access parent has the same right as a custodial parent (barring a court order to the contrary) to, among other things, “make inquires and to be given information as to the health, education and welfare of the child”.
- These rights would be exercised by making a request for disclosure (as opposed to an “access request” under s.52) to a HIC having custody or control of the child’s information.



PHIPA OVERVIEW

DO NOT RELEASE WITHOUT MY CONSENT

- Under PHIPA, the psychologist's or psychiatrist's consent would not be required. If the individual or their substitute decision-maker consents to the disclosure, this is sufficient.



PHIPA OVERVIEW

DO NOT RELEASE WITHOUT MY CONSENT

- There is no requirement to consult the psychologist or the psychiatrist, if the agency is the HIC.
- However, if there is a concern that one of the exemptions set out in s.52(1)(e) (assuming the individual or substitute decision maker were to make an access request, in order to obtain and then hand over the information to someone else.), especially (iii) re: identifying a person who provided the information in confidence might apply and that practitioner might be the only person who could assess that properly, it may be a good practice to consult that practitioner.
- Subsection 52(5) explicitly provides that, before deciding to refuse to grant an individual access to a record of PHI under subclause (1)(e)(i) (risk of harm), a custodian **may** consult with a member of the College of Physicians and Surgeons of Ontario or a member of the College of Psychologists of Ontario.



PHIPA OVERVIEW

COMBINED FILES

- PHIPA doesn't speak directly to this issue, but if the parent's information is put in the same file as the child's, then arguably the child would have a right of access to that information when requesting his or her file under PHIPA, as it would be considered to be part of the child's PHI.
- As a corollary, each parent who is allowed access to the file may have access to that information about the other parent
- A best practice would be to keep the files separate, but indicate in each a link to the other, if desirable.



PHIPA OVERVIEW

KINSHIP CARE

- The basic rule is that PHI can be disclosed between “health information custodians” on the basis of implied consent, if it is being disclosed for the purpose of health care or assisting in providing health care.
- If the Kinship Care providers are not custodians or their reasons for disclosure are not for health care, these limitations must be kept in mind. If they actually have custody, then their right to information would be like that of parents.



PHIPA OVERVIEW

THE EXEMPTIONS TO RIGHT OF ACCESS

- The right of access in s.52 of PHIPA is subject to exemptions.
- A relevant exemption in this context might be 52(1)(b) i.e. an individual has a right of access to a record of PHI about the individual unless, “another Act, an Act of Canada or a court order prohibits the disclosure to the individual of the record or the information in the record in the circumstances.”



PHIPA SCENARIOS

FACTUAL SITUATION #1

- A 7 year old child is referred by his school to a children's mental health clinic because of behavioural problems at school and in the home. The family participated in the initial assessment which resulted in a decision to provide in-home service. A Child and Youth Worker (CYW) visits with mother and child to work on behavioural problems in the home. On several occasions, father is at home during CYW visits. Father confides in CYW that he's depressed, and concerned he may lose his job; mother is not home during these discussions.

CYW creates a file for the child and documents conversations with father. Later on mother makes an access request to see the file.



Issues: Access to Record, PHI

- **Q:** What should the CYW do?
- **Q:** Is the record 'dedicated primarily to' child, mother, father or family?
- **Q:** Is mother entitled to information about father?
- **Q:** Is father entitled to his information in the record?
- **Q:** Does child have access to this information? Can child have access in the future?
- **Q:** How can father's information be safeguarded?



PHIIPA SCENARIOS

FACTUAL SITUATION #2

- A clinician working at a large children's mental health centre realizes that one of the memory sticks he shares with colleagues in the department has gone missing. The clinician remembers that he left some client information including draft reports on it, but that was a month ago. The clinician suspects that someone in another department borrowed it and forgot to return it.



Issues: Access to Record, Phi

- **Q:** What should the clinician do?
- **Q:** What if the clinician can't recall which clients were identified in the reports?
- **Q:** How should the centre handle this situation?
- **Q:** What steps could the centre take to reduce the risk of this happening again?



PHIPA SCENARIOS

FACTUAL SITUATION #3

- A clinician is providing counseling to a 13 year old, during the course of treatment the clinician receives a psycho-educational report from an external psychologist. Three months later, the family is moving and requests that a copy of the child's file be sent to a new clinician.



Issues: Access to Record, Phi

- **Q:** Whose consent would you need to release the information on file?
- **Q:** Would you release the entire client file including external reports and case notes?
- **Q:** What if the external psycho-educational report states that it not be disclosed without the author's permission and must only be disclosed to another psychologist?



PHIPA SCENARIOS

FACTUAL SITUATION #4

- During residential licensing, the ministry representative asks to review the records of all clients receiving this service. One of the clients who is 16 years old and knows all about PHIPA says to the residential supervisor that he does not consent to the ministry representative reviewing his file.



Issues: Access to Record, Phi

- **Q:** What do you do?
- **Q:** Would it be different if the child was 10, 12?



PHIPA SCENARIOS

FACTUAL SITUATION #5

- The mother of an 11 year old child phones a mental health centre, she is directed to intake where she provides an intake worker with information about the child and completes the BCFPI. The intake worker schedules an assessment appointment 3 weeks from the intake call. At the end of the assessment appointment, recommendations are made to initiate individual counseling with the child as well as family counseling (parents and child together). The child is willing to attend the counseling sessions but doesn't want her information shared with anyone. During the course of treatment a psychological assessment is carried out. Three months later, the mother is approached by the school for a copy of the psychology report.



Issues: collection, use of information, consent

- **Q:** What should the clinician do?
- **Q:** Whose consent is required to release the report?
- **Q:** Do the parents have any right to access the file during the course of treatment or at any time?



PHIPA SCENARIOS

FACTUAL SITUATION #6

- The Smiths came to AB Centre for service in December 2004 for their child Peter (age 11 at the time of service). Peter and his family successfully completed service 6 months later. In June the Smiths come back for service but this time it is for their child Paul (age 7). When the clinician picking up the case learns that the family has been to the centre before, she decides that before she meets with Paul and his family, she can get a head start by reviewing Peter's record as she is sure it contains all sorts of family background. During supervision, she tells this to her supervisor.



Issues: collection, use, access, custody and control

- **Q:** What should the supervisor tell the clinician about this behaviour?
- **Q:** What responsibilities do health information custodians have to protect client information?



PHIPA SCENARIOS

FACTUAL SITUATION #7

- A clinician is working with a 16 year old boy who is diagnosed with Asperger's syndrome by the psychiatrist at the centre. The parents are divorced (not an amicable split) and dad is now requesting a copy of the assessment (dad was not part of the assessment process). At intake the mother reported having full custody. There had been some question about this until recently when the clinician asked for and received a copy of the custody agreement. The clinician established that the parents have joint custody. During the course of the psychiatric assessment, information was collected about the mother and now she has some concerns that if dad has this information he may use it against her in court to gain full custody of the boy. Mom requests that the information about her not be shared.



Issues: lockbox, custody, corrections

Q: Is it possible to respect mom's request and provide a copy of the assessment to dad with the information that is specific to mom blacked out?

Q: Would this matter if the information in the psychiatric report which the mother did not want shared was her disagreement with the diagnosis?



How to Contact Us

Ken Anderson, Assist Commissioner (Privacy)

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca